UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590 02/07/2006

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/700,656	VATER ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) *1-25,34-41 and 43* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-33, 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election of Group II, Claims 26-33 and 42, in the reply filed on 16 November 2005 is acknowledged. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (MPEP § 818.03(a)). Specifically, Applicant's reply appears to be directed to the comments made by the Examiner under the heading "Response to Arguments" in the Office action mailed 17 October 2005; however, Applicant has not addressed the reasoning of the actual requirement for restriction, regarding the differing special technical features of the inventions of Groups I, II, and III (set forth under the heading "Election/Restrictions" in the Office action mailed 17 October 2005).

2. Claims 1-25, 34-41, and 43 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to nonelected inventions, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 16 November 2005.

Response to Arguments

3. Applicant's arguments with respect to claims 26-33 and 42 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 28-30, 33, and 42 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 28 recites the limitations "the memory" and "the data carrier". There is insufficient antecedent basis for these limitations in the claims.

Claims 30 and 33 each recite the limitation "the combination"; however, it is unclear whether this is intended to refer to the combination that falsifies or the combining in order to compensate for the falsification (see Claim 26), or to both. For purposes of applying the art, the combination recited in Claim 30 is assumed to refer to the compensating combination, and the combination recited in Claim 33 is assumed to refer to either of the two combinations.

Claim 42 recites the limitation "the security-relevant operations". There is insufficient antecedent basis for this limitation in the claims, although it appears to refer to the "one or more operations" of Claim 26.

Claim 29 is rejected due to its dependence on rejected Claim 28.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 26-32 and 42 are rejected under 35 U.S.C. 102(e) as being anticipated by Jakobsson, US Patent 6049613 (previously cited in the Office actions mailed 23 July 2004 and 22 February 2005).

In reference to Claim 26, Jakobsson discloses a method of protecting secret data, where the method includes falsifying input data by combination with auxiliary data (column 5, line 56-column 6, line 42; column 6, line 56-column 7, line 3), and combining the output data with an auxiliary function value in order to compensate for the falsification of the input data, where the auxiliary value was previously determined (column 7, lines 48-65; column 10, lines 5-6).

In reference to Claim 27, Jakobsson further discloses that the combination with the auxiliary function value is performed before execution of a non-linear operation (column 7, lines 48-65, where this is performed before execution of the operation at column 7, 66-column 8, line 28).

In reference to Claim 28, Jakobsson further discloses that the auxiliary data are varied (column 6, lines 33-42, where different keys are used).

In reference to Claims 29-32, Jakobsson further discloses that new auxiliary values can be generated by combining existing values, that auxiliary data are selected randomly, pairs of auxiliary data and auxiliary function values are generated, and the auxiliary data are random numbers (column 6, lines 33-42; column 7, lines 18-21, where keys are randomly chosen).

In reference to Claim 42, Jakobsson further discloses that operations include permutations of data (see column 6, lines 50-55; column 7, lines 29-33).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jakobsson.

Jakobsson discloses everything as applied to Claim 26. Jakobsson further discloses various encryption methods (column 6, lines 11-42; column 1, lines 19-50); however, Jakobsson does not explicitly disclose combining data using an XOR operation. Official notice is taken that it is well known in the art to use XOR for an easily executed encryption operation combining data with a key. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use XOR for the combination operation in order to take advantage of the simplicity of the operation.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER